

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2003-114806

(P2003-114806A)

(43) 公開日 平成15年4月18日(2003.4.18)

(51) Int.Cl.⁷

G 0 6 F 11/00

識別記号

F I

G 0 6 F 9/06

テーマコード(参考)

6 3 0 A 5 B 0 7 6

審査請求 未請求 請求項の数10 O L (全 13 頁)

(21) 出願番号 特願2001-308156(P2001-308156)

(22) 出願日 平成13年10月4日(2001.10.4)

(71) 出願人 000005108

株式会社日立製作所

東京都千代田区神田駿河台四丁目6番地

(72) 発明者 大島 剛

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(72) 発明者 木村 信二

神奈川県川崎市麻生区王禅寺1099番地 株

式会社日立製作所システム開発研究所内

(74) 代理人 100083552

弁理士 秋田 収喜

最終頁に続く

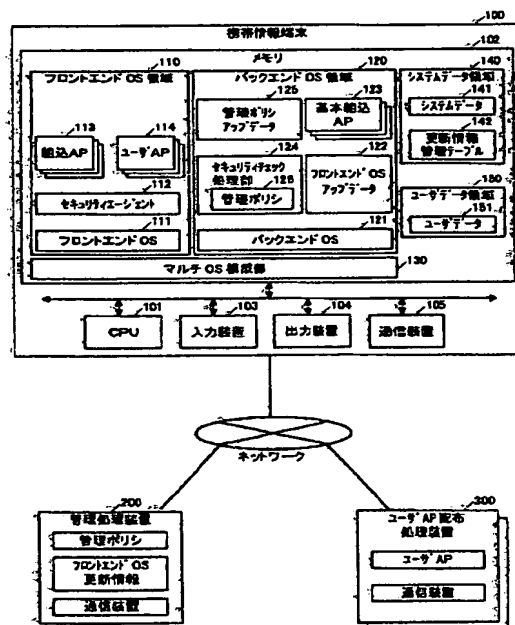
(54) 【発明の名称】 OS更新方法及びセキュリティ制御方法並びにその実施装置

(57) 【要約】

【課題】 情報処理装置のOSの更新を効率良く行うことが可能な技術を提供する。

【解決手段】 情報処理装置内にインストールされているOSを更新するOS更新方法において、通常のアプリケーション処理を制御するフロントエンドOSの更新が必要であるかどうかを判定するステップと、前記フロントエンドOSの更新が必要であると判定された場合に、動作中のフロントエンドOSの処理を終了させて情報処理装置の制御をバックエンドOSに切り換えるステップと、フロントエンドOSを最新の状態に更新する為の更新データをバックエンドOSの制御下で取得してフロントエンドOSを最新の状態に更新するステップと、前記最新の状態に更新されたフロントエンドOSを再起動するステップとを有するものである。

図 1



1

【特許請求の範囲】

【請求項1】 情報処理装置内にインストールされているOSを更新するOS更新方法において、通常のアプリケーション処理を制御するフロントエンドOSの更新が必要であるかどうかを判定するステップと、前記フロントエンドOSの更新が必要であると判定された場合に、動作中のフロントエンドOSの処理を終了させて情報処理装置の制御をバックエンドOSに切り換えるステップと、フロントエンドOSを最新の状態に更新する為の更新データをバックエンドOSの制御下で取得してフロントエンドOSを最新の状態に更新するステップと、前記最新の状態に更新されたフロントエンドOSを再起動するステップとを有することを特徴とするOS更新方法。

【請求項2】 フロントエンドOSの制御下で取得または作成されたデータをフロントエンドOSの格納領域とは異なる領域に格納し、更新前のフロントエンドOSの制御下で取得または作成されたデータを更新後のフロントエンドOSの制御下で再利用することを特徴とする請求項1に記載されたOS更新方法。

【請求項3】 前記切り換えられたバックエンドOSの制御下で必要最小限のアプリケーション処理を実行することを特徴とする請求項1または請求項2のいずれかに記載されたOS更新方法。

【請求項4】 情報処理装置内で実行されるアプリケーション処理のセキュリティを制御するセキュリティ制御方法において、情報処理装置上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せを行うステップと、前記問合せの行われた処理要求が許可されているかどうかを管理ポリシーに従って判定した後、その判定内容を示す問合せ結果を応答するステップと、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行するステップとを有することを特徴とするセキュリティ制御方法。

【請求項5】 アプリケーションの処理要求が行われたOSとは異なるOSの制御下で前記管理ポリシーを管理することを特徴とする請求項4に記載されたセキュリティ制御方法。

【請求項6】 管理処理装置内に格納された管理ポリシーの内容に従って情報処理装置内の管理ポリシーを更新することを特徴とする請求項4または請求項5のいずれかに記載されたセキュリティ制御方法。

【請求項7】 前記問合せは、当該アプリケーションプログラムの実行可否、当該アプリケーションによる端末内の情報へのアクセス可否、外部との通信可否を問合せるものであることを特徴とする請求項4乃至請求項6のいずれか1項に記載されたセキュリティ制御方法。

【請求項8】 装置内にインストールされているOSを

2

更新する情報処理装置において、

通常のアプリケーション処理を制御するフロントエンドOSの更新が必要であるかどうかを判定し、フロントエンドOSを最新の状態に更新する為の更新データをバックエンドOSの制御下で取得してフロントエンドOSを最新の状態に更新するフロントエンドOSアップデータと、

前記フロントエンドOSの更新が必要であると判定された場合に、動作中のフロントエンドOSの処理を終了させて情報処理装置の制御をバックエンドOSに切り換えた後、前記最新の状態に更新されたフロントエンドOSを再起動するマルチOS構成部とを備えることを特徴とする情報処理装置。

【請求項9】 装置内で実行されるアプリケーション処理のセキュリティを制御する情報処理装置において、情報処理装置上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せをセキュリティチェック処理部に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行するセキュリティエージェントと、前記問合せの行われた処理要求が許可されているかどうかを管理ポリシーに従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェントに応答するセキュリティチェック処理部とを備えることを特徴とする情報処理装置。

【請求項10】 管理処理装置内に格納された管理ポリシーの内容に従って情報処理装置内の管理ポリシーを更新する管理ポリシーアップデータを備えることを特徴とする請求項9に記載された情報処理装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明はオペレーティングシステム(OS)の更新、管理ポリシーに従ったセキュリティの実現及び管理ポリシーのリモートメンテナンスを行う情報処理装置に関し、特にOSの更新機能、セキュリティ機能及びリモートメンテナンス機能を複数のOSの搭載により提供する情報処理装置に適用して有効な技術に関するものである。

【0002】

【従来の技術】近年の携帯電話等の携帯情報端末の急速な進歩に伴い、インターネットにアクセスしたり、音楽データをダウンロードして再生したり、利用者の写真を撮影して電子メールとして送信する等、携帯情報端末によって様々な機能が提供されるようになってきている。

【0003】このような携帯情報端末では、携帯情報端末内の不揮発性メモリにOS、組込アプリケーションプログラム(組込AP)及びユーザアプリケーションプログラム(ユーザAP)やそれらの処理でアクセスされるデータを格納しておき、電源投入時や利用者からの操作が

行われたときに前記不揮発性メモリ上のプログラムを起動して各種機能を提供している。

【0004】前記従来の携帯情報端末において、新たに機能追加を行う場合や既存のプログラムの修正を行う場合には前記不揮発性メモリ上のプログラムを更新する必要があるが、携帯情報端末内の不揮発性メモリ上のプログラムを更新する場合、携帯情報端末をパーソナルコンピュータ（PC）等の専用の情報処理装置に接続し、その情報処理装置の動作によって携帯情報端末内の不揮発性メモリの内容を書き換える必要があり、一般のユーザが行うのは困難である為、端末本体をサービスセンタに持ち込んでプログラムの書き換えを行っている。またその際の費用は端末提供者によって負担されている。

【0005】一方、高性能化、多機能化する携帯情報端末では、ユーザAPをダウンロードして実行できる携帯情報端末が増えているが、アプリケーション処理の実行の際に携帯情報端末内にある情報にアクセスできるかどうかや、外部との通信を行えるかどうかといったセキュリティに関する設定は、その携帯情報端末を提供しているサービス事業者側によって全て行われている。

【0006】例えば、一般消費者向けのサービスを行っているサービス事業者は、端末内の住所録が外部に漏れることを防ぐ為、端末内の情報と外部に同時にアクセスできるアプリケーションを、サービス事業者自らが提供するアプリケーションだけに制限している。

【0007】なお、フラッシュメモリに記憶された、複数のプログラムブロックからなるプログラムデータの一部のプログラムブロックのデータを更新するプログラム更新装置およびプログラム更新方法については、特開2000-242487号公報に記載されている。その概要は、A～Eの各機能を実現するための複数のプログラムブロックを記憶したフラッシュメモリに対して、たとえば、機能DのOSデータを更新する場合、第4番目のメモリブロックのデータを消去する前に、機能DのOSデータとともに第4番目のメモリブロック内に格納された、機能CのOSデータの一部と機能EのOSデータの一部のデータを、パーソナルコンピュータに一時的に退避し、第4番目のメモリブロックのデータを消去した後、新しい機能DのOSデータとともに退避データを第4番目のメモリブロックの元の位置に書き込むものである。

【0008】

【発明が解決しようとする課題】前記従来の携帯情報端末では、OSや組込AP等の更新を利用者側で行うことが困難であり、端末本体をサービスセンタに持ち込んでプログラムの書き換えを行う必要がある為、OSや組込APの更新作業に多大な時間と莫大な費用を要するという問題がある。今後、携帯情報端末の高機能化、高性能化に伴って、バグの発生という問題は益々多くなると考えられる為、このプログラムの更新時の問題を解決する

必要がある。

【0009】一方、高性能化、多機能化する携帯情報端末では、今後、現在のPCの様にビジネスの世界に進出することが予想されるが、現状の携帯情報端末のセキュリティは、その携帯情報端末を提供しているサービス事業者側で全て設定されている為、企業がこれを利用する場合、自分たちが設定した業務用のアプリケーションも端末内外の情報にアクセスできる様にする等のサービス事業者とは異なる基準でアプリケーションのアクセス可否を決定することができないという問題がある。

【0010】また、前記従来の携帯情報端末において、サービス事業者が企業側の要求に沿ってアクセス可否の情報を設定したとしても、一旦設定されたアプリケーションのアクセス可否の様な情報は端末内の不揮発性メモリに記憶されており、この情報を更新するリモートメンテナンス等の有効な手段が提供されていない為、業務内容の変化に応じて業務用アプリケーションの機能を変更する度に端末を回収して、専用の装置を使って業務用アプリケーション及び対応するセキュリティ情報を更新する必要がある、業務用アプリケーション及びそのセキュリティ情報のメンテナンスに大きな時間と費用がかかるという問題がある。

【0011】本発明の目的は上記問題を解決し、情報処理装置のOSの更新を効率良く行うことが可能な技術を提供することにある。本発明の他の目的は情報処理装置で利用者独自の基準に基づいたセキュリティ機能を実現することが可能な技術を提供することにある。本発明の他の目的は情報処理装置内のセキュリティ機能をリモートメンテナンスすることが可能な技術を提供することにある。

【0012】

【課題を解決するための手段】本発明は、装置内にインストールされているOSを更新する情報処理装置において、フロントエンドOSの更新が必要であると判定された場合にバックエンドOSの制御下でフロントエンドOSの更新を行うものである。

【0013】本発明では、携帯電話等の携帯情報端末である情報処理装置からネットワークを介して管理処理装置へアクセスし、通常のアプリケーション処理を制御するフロントエンドOSの更新情報を管理処理装置から取得して、情報処理装置内にインストールされているフロントエンドOSの管理情報と前記取得した更新情報とを比較し、情報処理装置内にインストールされているフロントエンドOSの更新が必要であるかどうかを判定する。

【0014】前記フロントエンドOSの更新が必要であると判定された場合には、マルチOS構成部の処理により、動作中のフロントエンドOSの処理を終了させて情報処理装置内の各部の制御をバックエンドOSに切り換えることによってバックエンドOSの制御下での情報処

5

理装置の動作を可能とした後、ネットワークを介して管理処理装置へアクセスし、フロントエンドOSを最新の状態に更新する為の更新データをバックエンドOSの制御下で管理処理装置から取得してフロントエンドOSを最新の状態に更新する。

【0015】そして、前記最新の状態に更新されたフロントエンドOSを再起動した後、情報処理装置内の各部の制御を更新後のフロントエンドOSに切り換えて、更新後のフロントエンドOSの制御による情報処理装置の動作を可能とする。

【0016】以上の様に本発明の情報処理装置によれば、フロントエンドOSの更新が必要であると判定された場合にバックエンドOSの制御下でフロントエンドOSの更新を行うので、情報処理装置のOSの更新を効率良く行うことが可能である。

【0017】

【発明の実施の形態】以下にOSの更新機能、セキュリティ機能及びリモートメンテナンス機能を複数のOSの搭載により提供する一実施形態の情報処理装置について説明する。

【0018】図1は本実施形態の携帯情報端末マルチOSシステムの概略構成を示す図である。図1に示す様に本実施形態の携帯情報端末マルチOSシステムは、携帯情報端末100と、管理処理装置200と、ユーザAP配布処理装置300とを有している。

【0019】携帯情報端末100は、管理処理装置200からフロントエンドOS更新情報や管理ポリシーを取得し、OSの更新機能、セキュリティ機能及びリモートメンテナンス機能を実現する携帯電話等の携帯型の情報処理装置である。

【0020】管理処理装置200は、フロントエンドOS更新情報や管理ポリシーについて、それらの最新情報を携帯情報端末100へ提供する処理装置である。ユーザAP配布処理装置300は、携帯情報端末100からの要求に応じてユーザAPを携帯情報端末100へ配布する処理装置である。

【0021】携帯情報端末100は、CPU101と、メモリ102と、入力装置103と、出力装置104と、通信装置105と、フロントエンドOS領域110と、バックエンドOS領域120と、管理ポリシー126と、システムデータ領域140と、システムデータ141と、更新情報管理テーブル142と、ユーザデータ領域150と、ユーザデータ151とを有している。

【0022】CPU101は、携帯情報端末100全体の動作を制御する装置である。メモリ102は、携帯情報端末100全体の動作を制御する際にその為の各種処理プログラムやデータをロードするフラッシュメモリ等の不揮発性の記憶装置である。

【0023】入力装置103は、携帯情報端末100を操作する為の各種入力を行う装置である。出力装置10

6

4は、携帯情報端末100の操作に伴う各種出力を行う装置である。通信装置105は、インターネットやイントラネット等のネットワークを介して他の処理装置との通信を行うと共に音声通話も行う装置である。

【0024】フロントエンドOS領域110は、フロントエンドOS111及びその制御下で動作する各種プログラムを格納する領域である。バックエンドOS領域120は、バックエンドOS121及びその制御下で動作する各種プログラムを格納する領域である。管理ポリシー126は、携帯情報端末100上で実行が許可されているアプリケーション処理の内容を示すデータである。

【0025】システムデータ領域140は、システムデータ141を格納する領域である。システムデータ141は、フロントエンドOS111、バックエンドOS121及びマルチOS構成部130等のシステムプログラムが動作する際に用いられるデータである。更新情報管理テーブル142は、フロントエンドOS111及び組込AP113の更新情報を格納するテーブルである。

【0026】ユーザデータ領域150は、ユーザデータ151を格納する領域である。ユーザデータ151は、ユーザAP114等のアプリケーション処理で取得または作成された住所録データや予定表データ等のデータである。

【0027】また携帯情報端末100は、フロントエンドOS111と、セキュリティエージェント112と、組込AP113と、ユーザAP114と、バックエンドOS121と、フロントエンドOSアップデート122と、基本組込AP123と、セキュリティチェック処理部124と、管理ポリシーアップデート125と、マルチOS構成部130とを有している。

【0028】フロントエンドOS111は、組込AP113やユーザAP114等の通常のアプリケーション処理を制御するOSである。セキュリティエージェント112は、携帯情報端末100上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されているかどうかの問合せをセキュリティチェック処理部124に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行する処理部である。

【0029】組込AP113は、フロントエンドOS111に組み込まれた住所録編集処理等の所定のアプリケーション処理を実行する処理部である。ユーザAP114は、ユーザAP配布処理装置300から配布された見直し処理等の所定のアプリケーション処理を実行する処理部である。

【0030】バックエンドOS121は、フロントエンドOS111の停止中に携帯情報端末100の動作を制御し、セキュリティチェック処理の際、セキュリティエージェント112からの処理要求に答えて動作するOSである。

10

20

30

40

50

【0031】フロントエンドOSアップデート122は、通常のアプリケーション処理を制御するフロントエンドOS111の更新が必要であるかどうかを判定し、フロントエンドOS111を最新の状態に更新する為の更新データをバックエンドOS121の制御下で取得してフロントエンドOS111を最新の状態に更新する処理部である。

【0032】基本組込AP123は、組込AP113の中で携帯電話として動作する為の必要最低限のサブセットであり、例えば組込AP113に住所録AP、着メロ作成AP、ゲームAPがあった場合、閲覧とそれによる電話のみが行える住所録APだけが入っており、バック

エンドOS121側にバグが入り込む余地をなるべく少なくした処理部である。

【0033】セキュリティチェック処理部124は、前記問合せの行われた処理要求が許可されているかどうかを管理ポリシー126に従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェント112に

応答する処理部である。管理ポリシーアップデート125は、管理処理装置200内に格納された管理ポリシーの内容に従って携帯情報端末100内の管理ポリシー126を

更新する処理部である。

【0034】マルチOS構成部130は、フロントエンドOS111及びバックエンドOS121をタイムスライスで動作させてフロントエンドOS111上のセキュリ

ティエージェント112とバックエンドOS121上のセキュリティチェック処理部124との間の通信を制御し、フロントエンドOS111の更新が必要であると判定された場合に、動作中のフロントエンドOS111の処理を終了させて携帯情報端末100の制御をバック

エンドOS121に切り換えた後、前記最新の状態に更新されたフロントエンドOS111を再起動する処理部である。

【0035】携帯情報端末100をフロントエンドOS111、セキュリティエージェント112、組込AP113、ユーザAP114、バックエンドOS121、フロントエンドOSアップデート122、基本組込AP123、セキュリティチェック処理部124、管理ポリシーアップデート125及びマルチOS構成部130として機能させる為のプログラムは、フラッシュメモリ等の記

録媒体に記録されて実行されるものとする。なお前記プログラムを記録する記録媒体はフラッシュメモリ以外の他の記録媒体でも良い。また前記プログラムを当該記録媒体から情報処理装置にインストールして使用しても良いし、ネットワークを通じて当該記録媒体にアクセスして前記プログラムを使用するものとしても良い。

【0036】本実施形態の携帯情報端末100では、組込AP113やユーザAP114等の通常のアプリケーション処理を制御するフロントエンドOS111と、フ

ロントエンドOS111の停止中に携帯情報端末100の動作を制御するバックエンドOS121とがタイムスライスで動作するマルチOSの構成をとっており、フロントエンドOS111として優れたGUI(Graphical User Interface)を備える最新のOSをインストールし、バックエンドOS121として動作の安定している以前のバージョンのOSを用いて携帯情報端末100を動作させているものとする。ここで、バックエンドOS121として、安定動作することが判っている別のOSを使ったり、同じバージョンでも機能を大きく制限することによって安定させたOSを用いても良い。

【0037】フロントエンドOS111に新しい機能を追加する場合や、フロントエンドOS111の新たに発見された不具合を修正する場合には、マルチOS構成部130により携帯情報端末100の入力装置103、出力装置104及び通信装置105を、フロントエンドOS111からバックエンドOS121に割り当てて動作させ、バックエンドOS121の制御下でフロントエンドOS111の更新を行う。ここで、マルチOS構成部130によるフロントエンドOS111からバックエンドOS121への切り替えは、フロントエンドOS111にマッピングされていたI/O処理の割り込みをバックエンドOS121にマッピングすることにより行うものとする。

【0038】以下に本実施形態の携帯情報端末マルチOSシステムにおいて、バックエンドOS121の制御下でフロントエンドOSアップデート122を動作させ、ネットワークを介して更新データをダウンロードして更新処理を実行し、フロントエンドOS111及び組込AP113を更新する処理について説明する。

【0039】図2は本実施形態のフロントエンドOSアップデート122の処理手順を示すフローチャートである。図2に示す様に本実施形態の携帯情報端末100のフロントエンドOSアップデート122は、通常のアプリケーション処理を制御するフロントエンドOS111の更新が必要であるかどうかを判定し、フロントエンドOS111を最新の状態に更新する為の更新データをバックエンドOS121の制御下で取得してフロントエンドOS111を最新の状態に更新する処理を行う。

【0040】ステップ201で携帯情報端末100のフロントエンドOSアップデート122は、前回の処理からの所定時間の経過や利用者から特定のキーが押された場合等、フロントエンドOS111の更新処理を開始する所定の条件が満たされたかどうかを調べ、前記条件が満たされている場合にはステップ202へ進む。

【0041】ステップ202では、携帯情報端末100にインストールされているフロントエンドOS111及び組込AP113の各種情報が格納されている更新情報管理テーブル142の内容を読み出す。

【0042】図3は本実施形態の更新情報管理テーブル142の一例を示す図である。図3に示す様に本実施形

10

20

30

40

50

態の更新情報管理テーブル142には、フロントエンドOS領域110に格納されているフロントエンドOS111及び組込AP113のバージョン、フロントエンドOS111及び組込AP113がフロントエンドOS領域110に格納された日付を示す更新日付、フロントエンドOS領域110での格納アドレスとその長さ、フロントエンドOS111及び組込AP113の更新情報を提供している管理処理装置200のアドレスを示す更新情報取得先URL (Uniform Resource Locator) が格納されている。

【0043】ステップ203でフロントエンドOSアップデータ122は、前記読み出した更新情報管理テーブル142中の更新情報取得先URLに示された管理処理装置200のアドレスにアクセスし、フロントエンドOS111及び組込AP113の更新情報の送信を管理処理装置200に要求する。

【0044】この更新情報の要求の際に、通信装置105がフロントエンドOS111に割り当てられており、バックエンドOS121に割り当てられていない場合には、フロントエンドOS111からバックエンドOS121への通信装置105の接続の切り換え要求をマルチOS構成部130に対して行うものとする。なおバックエンドOS121としてリアルタイム処理に優れたOSを採用し、通信処理に関しては常にバックエンドOS121が行っているものとしても良い。

【0045】管理処理装置200は、フロントエンドOS111及び組込AP113の更新情報の取得要求を携帯情報端末100から受信すると、管理処理装置200内に格納されているフロントエンドOS更新情報を読み出し、携帯情報端末100へ送信する。ここで管理処理装置200のフロントエンドOS更新情報には、最新のフロントエンドOS111及び組込AP113のバージョン及び更新日付が格納されているものとする。

【0046】携帯情報端末100のフロントエンドOSアップデータ122は、管理処理装置200からフロントエンドOS更新情報を受信するとステップ204に進み、更新情報管理テーブル142中に格納されているフロントエンドOS111及び組込AP113のバージョン及び更新日付と、管理処理装置200から受信したフロントエンドOS更新情報中のバージョン及び更新日付とを比較し、更新情報管理テーブル142中に格納されているバージョン及び更新日付の方が古い場合には、更新処理が必要であるものとしてステップ205へ進む。

【0047】ステップ205では、バックエンドOS121を介してマルチOS構成部130を呼び出し、フロントエンドOS111及び組込AP113の終了をマルチOS構成部130に要求する。

【0048】マルチOS構成部130は、フロントエンドOS111及び組込AP113の終了要求をフロントエンドOSアップデータ122から受け取ると、動作中

のフロントエンドOS111及び組込AP113の処理を終了させた後、入力装置103、出力装置104及び通信装置105等のリソースをバックエンドOS121に割り当て、携帯情報端末100の制御をバックエンドOS121に切り換える。

【0049】ここで利用者からアプリケーション処理の実行要求が入力された場合には、バックエンドOS121を介して基本組込AP123を動作させることにより、フロントエンドOS111の更新中でも必要最小限の処理を行うものとする。

【0050】またシステムデータ141やユーザデータ151は、フロントエンドOS領域110とは異なるシステムデータ領域140やユーザデータ領域150に格納されているので、必要最小限の処理を提供するバックエンドOS121や基本組込AP123は、フロントエンドOS111で用いられていたシステムデータ141やユーザデータ151をそのまま利用してフロントエンドOS111及び組込AP113と同様の処理を利用者に提供することができる。

【0051】ステップ206でフロントエンドOSアップデータ122は、前記読み出した更新情報管理テーブル142中の更新情報取得先URLに示された管理処理装置200のアドレスにアクセスし、フロントエンドOS111及び組込AP113を最新の状態に更新する為の更新データの送信を管理処理装置200に要求する。

【0052】ここで前記更新データは、フロントエンドOS111及び組込AP113を最新の状態に更新する為のインストールプログラムまたは差分データ、或いは最新のフロントエンドOS111及び組込AP113そのもののいずれであっても良いものとする。

【0053】ステップ207でフロントエンドOSアップデータ122は、管理処理装置200から送信された更新データを受信し、その更新データを用いて、更新情報管理テーブル142中の格納アドレス及び長さで示された領域に格納されているフロントエンドOS111及び組込AP113を最新の状態に更新した後、更新情報管理テーブル142中のバージョン、更新日付等の情報を新しい内容に更新する。

【0054】ステップ208では、バックエンドOS121を介してマルチOS構成部130を呼び出し、フロントエンドOS111及び組込AP113の再起動を指示する。

【0055】マルチOS構成部130は、フロントエンドOS111及び組込AP113の再起動指示をフロントエンドOSアップデータ122から受け取ると、更新後のフロントエンドOS111及び組込AP113を再起動させた後、入力装置103、出力装置104及び通信装置105等のリソースをフロントエンドOS111に割り当て、携帯情報端末100の制御をフロントエンドOS111に切り換える。

【0056】従来の携帯情報端末では、不揮発性メモリに格納されているOSや組込APを実行させることにより動作している為、OSや組込APの更新を行う際に更新対象のOSや組込APの動作を停止させる必要があるが、OSを停止させると携帯情報端末単独では動作できなくなる為、端末本体をサービスセンタに持ち込んで専用の装置に接続し、プログラムの書き換えを行う必要があった。

【0057】これに対し、本実施形態の携帯情報端末マルチOSシステムでは、更新対象のフロントエンドOS 111及び組込AP 113を停止させた後、携帯情報端末100の制御をバックエンドOS 121に移し、バックエンドOS 121の制御下でフロントエンドOSアップデート122を動作させるので、ネットワークを介して更新データをダウンロードして更新処理を実行し、オンラインでフロントエンドOS 111及び組込AP 113の更新を行うことができる。

【0058】本実施形態では、OSや組込APを不揮発性メモリに格納している携帯情報端末100においてフロントエンドOS 111及び組込AP 113を更新する処理について説明したが、磁気ディスク装置に格納されたOSや組込APをメモリにロードして実行するPC等の情報処理装置に適用しても良い。

【0059】従来の情報処理装置では、CD-ROM等の可搬型の記録媒体を用い、人手を介してプログラムの更新が行われているが、本実施形態では、ネットワークを介してオンラインで更新処理を行うので、人手を介すること無く更新処理を効率的に行うことが可能である。

【0060】また従来の情報処理装置では、更新処理用の記録媒体の内容をネットワーク経由で取得してオンラインで更新処理を行うことも考えられるが、OSや組込APの不具合を修正する目的で更新処理を行う場合、シングルOS環境下では不具合の有るOSや組込APを用いて通信処理を行うことになる為、その不具合により通信処理が正常に実行できず、更新処理を行えない可能性がある。

【0061】これに対して本実施形態では、不具合のあるフロントエンドOS 111及び組込AP 113を停止し、動作の安定しているバックエンドOS 121の制御下で更新処理を行うので、更新対象の不具合に影響されることが無く更新処理を効率的に行うことが可能である。

【0062】次に、本実施形態の携帯情報端末マルチOSシステムにおいて、バックエンドOS領域120中の管理ポリシー126に従ったセキュリティ機能を実現する処理について説明する。

【0063】図4は本実施形態のセキュリティエージェント112の処理手順を示すフローチャートである。図4に示す様に本実施形態のセキュリティエージェント112は、携帯情報端末100上でアプリケーションの処理要求が行われた場合に、その処理要求が許可されてい

るかどうかの問合せをセキュリティチェック処理部124に送り、前記問合せ結果の内容が当該アプリケーション処理の実行許可を示している場合にそのアプリケーション処理を実行する処理を行う。

【0064】ステップ401で携帯情報端末100のセキュリティエージェント112は、携帯情報端末100上で行われたアプリケーションの処理要求の内容を調べ、その処理要求がアプリケーション処理の起動要求である場合にはステップ402へ進む。

【0065】ステップ402では、その起動要求の行われたアプリケーションの名称を指定し、そのアプリケーション処理の実行が許可されているかどうかの問合せを、フロントエンドOS 111、マルチOS構成部130及びバックエンドOS 121を経由してセキュリティチェック処理部124に送る。

【0066】図5は本実施形態のセキュリティチェック処理部124の処理手順を示すフローチャートである。図5に示す様に本実施形態のセキュリティチェック処理部124は、セキュリティエージェント112から問合せの行われた処理要求が許可されているかどうかを管理ポリシー126に従って判定した後、その判定内容を示す問合せ結果をセキュリティエージェント112に回答する処理を行う。

【0067】ステップ501で携帯情報端末100のセキュリティチェック処理部124は、セキュリティエージェント112からの問合せの内容を調べ、その問合せ内容がアプリケーション処理の実行が許可されているかどうかの問合せである場合にはステップ502へ進む。

【0068】ステップ502では、管理ポリシー126を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するAP名のレコードから更新指示の内容を読み出して、そのアプリケーションの更新指示が有るかどうかを調べ、更新指示の内容が「有」であり更新指示の有ることを示している場合にはステップ503へ進む。

【0069】図6は本実施形態の管理ポリシー126の一例を示す図である。図6に示す様に本実施形態の管理ポリシー126は、最新の管理ポリシーの取得先のURLを示す管理ポリシー取得先URLと、管理ポリシー126が前回更新された日付を示す更新日付と、セキュリティチェック処理部124によりチェックが行われるアプリケーション処理の名称を示すAP名の項目と、そのアプリケーションの更新が指示されているかどうかを示す更新指示と、そのアプリケーション処理を実行することが許可された期限を示す有効期限と、そのアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されているかどうかを示す情報アクセスの項目と、そのアプリケーション処理による外部への通信処理が許可されているかどうかを示す通信の項目を有している。

【0070】ステップ503では、ユーザAP配布処理

13

装置300へアクセスし、前記問合せの行われたアプリケーションの最新バージョンをユーザAP配布処理装置300から取得してユーザAP114の更新処理を行い、管理ポリシ126中の前記レコードの更新指示の内容を「無」に変更する。

【0071】ステップ504では、管理ポリシ126を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するAP名のレコードから有効期限を読み出す。

【0072】ステップ505では、管理ポリシ126から読み出した有効期限と現在の日付とを比較し、現在の日付が前記有効期限内であり前記問合せの行われたアプリケーションが有効である場合にはステップ506へ進み、そのアプリケーション処理の実行が許可されていることを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0073】またステップ505で管理ポリシ126の有効期限と現在の日付とを比較した結果、現在の日付が前記有効期限を経過しており、前記問合せの行われたアプリケーションが有効ではない場合にはステップ507へ進み、そのアプリケーション処理の実行が許可されていないことを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0074】ステップ403でセキュリティエージェント112は、セキュリティチェック処理部124から返された問合せ結果を参照し、そのアプリケーション処理の実行が許可されていることを示す問合せ結果を受け取っている場合にはステップ404へ進み、そうでない場合には実行が許可されていないことを示すメッセージを出力装置104へ出力する。

【0075】ステップ404では、前記アプリケーション処理の起動要求をフロントエンドOS111に対して行ってそのアプリケーションを起動し、その起動されたアプリケーションのプロセスを識別する為の識別情報であるプロセスIDをフロントエンドOS111から取得する。

【0076】ステップ405では、フロントエンドOS111から前記取得したプロセスIDと前記起動要求の行われたアプリケーションの名称を対応付けてメモリ102内に格納する。

【0077】一方、ステップ401でアプリケーションの処理要求の内容を調べた結果、その処理要求がアプリケーション処理の起動要求ではない場合にはステップ406へ進む。

【0078】ステップ406では、携帯情報端末100上で行われたアプリケーションの処理要求の内容が携帯情報端末100内のユーザデータ領域150に格納され

14

た住所録データや予定表データ等の情報へのアクセスであるかどうかを調べ、前記情報へのアクセスである場合にはステップ407へ進む。

【0079】ステップ407では、前記処理要求を行ったアプリケーション処理のプロセスIDを取得し、メモリ102内に前記格納したプロセスIDとアプリケーション名称の情報から、そのプロセスIDに対応するアプリケーションの名称を読み出す。

【0080】ステップ408では、前記読み出したアプリケーションの名称を指定し、そのアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されているかどうかの問合せを、フロントエンドOS111、マルチOS構成部130及びバックエンドOS121を経由してセキュリティチェック処理部124に送る。

【0081】ステップ501でセキュリティチェック処理部124は、セキュリティエージェント112からの問合せの内容を調べ、その問合せ内容がアプリケーション処理の実行が許可されているかどうかの問合せではない場合にはステップ508へ進む。

【0082】ステップ508では、セキュリティエージェント112からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されているかどうかの問合せである場合にはステップ509へ進む。

【0083】ステップ509では、管理ポリシ126を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するAP名のレコードから情報アクセスの項目を読み出す。

【0084】ステップ510では、管理ポリシ126から読み出した情報アクセスの項目内容を参照し、携帯情報端末100内の情報へのアクセスが許可されている場合にはステップ511へ進み、そのアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されていることを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0085】またステップ510で管理ポリシ126から読み出した情報アクセスの項目内容を参照した結果、携帯情報端末100内の情報へのアクセスが許可されていない場合にはステップ512へ進み、そのアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されていないことを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0086】ステップ409でセキュリティエージェント112は、セキュリティチェック処理部124から返された問合せ結果を参照し、そのアプリケーション処理

15

による携帯情報端末100内の情報へのアクセスが許可されていることを示す問合せ結果を受け取っている場合にはステップ410へ進み、そうでない場合にはその情報へのアクセスが許可されていないことを示すメッセージを出力装置104へ出力する。

【0087】ステップ410では、前記アプリケーション処理により行われた情報へのアクセス要求をフロントエンドOS111に対して行ってその情報へのアクセスを実行し、その処理結果をフロントエンドOS111から取得して当該アプリケーションに返す。

【0088】一方、ステップ406でアプリケーションの処理要求の内容を調べた結果、その処理要求が携帯情報端末100内の情報へのアクセス要求ではない場合にはステップ411へ進む。

【0089】ステップ411では、携帯情報端末100上で行われたアプリケーションの処理要求の内容が携帯情報端末100外部への通信要求であるかどうかを調べ、前記外部への通信要求である場合にはステップ412へ進む。

【0090】ステップ412では、前記処理要求を行ったアプリケーション処理のプロセスIDを取得し、メモリ102内に前記格納したプロセスIDとアプリケーション名称の情報から、そのプロセスIDに対応するアプリケーションの名称を読み出す。

【0091】ステップ413では、前記読み出したアプリケーションの名称を指定し、そのアプリケーション処理による携帯情報端末100外部への通信処理が許可されているかどうかの問合せを、フロントエンドOS111、マルチOS構成部130及びバックエンドOS121を経由してセキュリティチェック処理部124に送る。

【0092】ステップ501の処理の後、ステップ508でセキュリティチェック処理部124は、セキュリティエージェント112からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末100内の情報へのアクセスが許可されているかどうかの問合せではない場合にはステップ513へ進む。

【0093】ステップ513では、セキュリティエージェント112からの問合せの内容を調べ、その問合せ内容がアプリケーション処理による携帯情報端末100外部への通信処理が許可されているかどうかの問合せである場合にはステップ514へ進む。

【0094】ステップ514では、管理ポリシー126を参照し、前記問合せ中に指定されたアプリケーションの名称と一致するAP名のレコードから通信の項目を読み出す。

【0095】ステップ515では、管理ポリシー126から読み出した通信の項目内容を参照し、携帯情報端末100外部への通信処理が許可されている場合にはステップ516へ進み、そのアプリケーション処理による携帯

16

情報端末100外部への通信処理が許可されていることを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0096】またステップ515で管理ポリシー126から読み出した通信の項目内容を参照した結果、携帯情報端末100外部への通信処理が許可されていない場合にはステップ517へ進み、そのアプリケーション処理による携帯情報端末100外部への通信処理が許可されていないことを示す問合せ結果を、バックエンドOS121、マルチOS構成部130及びフロントエンドOS111を経由してセキュリティエージェント112に送る。

【0097】ステップ414でセキュリティエージェント112は、セキュリティチェック処理部124から返された問合せ結果を参照し、そのアプリケーション処理による携帯情報端末100外部への通信処理が許可されていることを示す問合せ結果を受け取っている場合にはステップ415へ進み、そうでない場合には外部への通信処理が許可されていないことを示すメッセージを出力装置104へ出力する。

【0098】ステップ415では、前記アプリケーション処理により行われた外部への通信要求をフロントエンドOS111に対して行って外部への通信処理を実行し、その処理結果をフロントエンドOS111から取得して当該アプリケーションに返す。

【0099】前記の様に本実施形態の携帯情報端末100では、携帯情報端末100上で行われたアプリケーションの処理要求をセキュリティエージェント112で受け取り、その処理要求が許可されているかどうかを管理ポリシー126に従ってセキュリティチェック処理部124で判定し、その判定結果に応じてアプリケーション処理を実行することにより携帯情報端末100でセキュリティ機能を提供しているため、管理ポリシー126にサービス事業者とは異なる基準でアプリケーションのアクセス可否の情報を設定することで、利用者である企業側の業務アプリケーションに適したセキュリティ機能を持たせることができる。

【0100】なお本実施形態では、アプリケーションの有効期限、携帯情報端末100内の情報アクセス、外部への通信処理に対するセキュリティ機能について説明したが、アプリケーション処理のバージョン毎に異なる有効期限を設定したり、携帯情報端末100内の住所録データや予定表データの情報毎に異なるアクセス可否データや、読み出し、書き込み、削除等のアクセス内容毎に異なる可否データを設定したり、通信先のURL毎に異なる可否データを設定する等、他の項目に対するセキュリティ機能を追加しても良い。

【0101】また、このセキュリティチェック処理及び管理ポリシー126の管理をバックエンドOS121の制

10

20

30

40

50

御下で行う様にするにより、フロントエンドOS 111が管理ポリシー126に直接アクセスすることがなくなるので、最新のフロントエンドOS 111に新たなセキュリティホールが発見された場合であっても、そのセキュリティホールによる管理ポリシー126への不正なアクセスを防止し、高いセキュリティを維持することができる。更に、フロントエンドOS領域110とバックエンドOS領域120とを異なる仮想メモリ空間とすることにより、フロントエンドOS 111からバックエンドOS領域120へ直接アクセスする処理を禁止すれば、更に高いセキュリティを提供することが可能である。

【0102】更に本実施形態の携帯情報端末100では、業務内容の変化に応じて業務用アプリケーションの機能を変更した場合に管理処理装置200内の管理ポリシーを変更しておき、管理ポリシーアップデータ125により、管理処理装置200内の管理ポリシーの内容に従って携帯情報端末100内の管理ポリシー126を更新することで、携帯情報端末100の管理ポリシー126をリモートメンテナンスすることができる。

【0103】図7は本実施形態の管理ポリシーアップデータ125の処理手順を示すフローチャートである。図7に示す様に本実施形態の管理ポリシーアップデータ125は、管理処理装置200内に格納された管理ポリシーの内容に従って携帯情報端末100内の管理ポリシー126を更新する処理を行う。

【0104】ステップ701で携帯情報端末100の管理ポリシーアップデータ125は、前回の処理からの所定時間の経過や利用者から特定のキーが押された場合等、管理ポリシー126の更新処理を開始する所定の条件が満たされたかどうかを調べ、前記条件が満たされている場合にはステップ702へ進む。

【0105】ステップ702では、携帯情報端末100に格納されている管理ポリシー126を参照し、最新の管理ポリシーの取得先のURLを示す管理ポリシー取得先URLと管理ポリシー126が前回更新された日付を示す更新日付を読み出す。

【0106】ステップ703で管理ポリシーアップデータ125は、前記読み出した管理ポリシー取得先URLに示された管理処理装置200のアドレスにアクセスし、管理処理装置200に格納されている管理ポリシーの更新情報の送信を管理処理装置200に要求する。

【0107】管理処理装置200は、管理ポリシーの更新情報の取得要求を携帯情報端末100から受信すると、管理処理装置200内に格納されている管理ポリシーが前回更新された日付を示す更新日付を読み出し、携帯情報端末100へ送信する。

【0108】携帯情報端末100の管理ポリシーアップデータ125は、管理処理装置200からフロントエンドOS更新情報を受信するとステップ704に進み、管理ポリシー126から読み出した更新日付と、管理処理装置

200から受信した更新日付とを比較し、携帯情報端末100に格納されている管理ポリシー126の更新日付の方が古い場合には、管理ポリシー126の更新処理が必要であるものとしてステップ705へ進む。

【0109】ステップ705では、バックエンドOS 121を介してセキュリティチェック処理部124に処理の一時停止指示を送り、セキュリティチェック処理部124に処理の一時停止を指示する。

【0110】セキュリティチェック処理部124は、処理の一時停止指示を管理ポリシーアップデータ125から受け取ると、現在処理中のセキュリティチェック処理を終了させた後、処理再開指示を待つ待ち状態に入る。

【0111】ステップ706で管理ポリシーアップデータ125は、前記読み出した管理ポリシー取得先URLに示された管理処理装置200のアドレスにアクセスし、最新の管理ポリシーデータの送信を管理処理装置200に要求する。

【0112】ステップ707で管理ポリシーアップデータ125は、管理処理装置200から送信された管理ポリシーデータを受信し、その管理ポリシーデータを用いて、管理ポリシー126を最新の状態に更新する。この際、更新された管理ポリシー126に示されているAP名とフロントエンドOS領域110に格納されているユーザAP 114の名称とを比較し、更新された管理ポリシー126内に、携帯情報端末100に格納されていない最新のユーザAPの情報が含まれている場合には、ユーザAP配布処理装置300へアクセスし、前記最新のユーザAPをダウンロードしてフロントエンドOS領域110のユーザAP 114の更新を行っても良い。また、更新された管理ポリシー126内にアプリケーションの更新指示が有る場合には、そのアプリケーションの更新処理をここで行っても良い。

【0113】ステップ708では、バックエンドOS 121を介してセキュリティチェック処理部124に処理の再開指示を送り、セキュリティチェック処理部124に処理の再開を指示する。

【0114】セキュリティチェック処理部124は、処理の再開指示を管理ポリシーアップデータ125から受け取ると、更新された管理ポリシー126を使用するセキュリティチェック処理を行える状態となる。

【0115】前記の様に本実施形態の携帯情報端末100では、業務内容の変化に応じて業務用アプリケーションの機能を変更した場合に管理処理装置200内の管理ポリシーを変更しておくことにより、携帯情報端末100内のユーザAP 114や管理ポリシー126のリモートメンテナンスを行うことが可能である。

【0116】以上説明した様に本実施形態の携帯情報端末によれば、フロントエンドOSの更新が必要であると判定された場合にバックエンドOSの制御下でフロントエンドOSの更新を行うので、携帯情報端末のOSの更

19

新を効率良く行うことが可能である。

【0117】また本実施形態の携帯情報端末によれば、管理ポリシーに従って許可されたアプリケーションの処理要求を実行するので、携帯情報端末で利用者独自の基準に基づいたセキュリティ機能を実現することが可能である。

【0118】また本実施形態の携帯情報端末によれば、管理処理装置内に格納された管理ポリシーの内容に従って携帯情報端末内の管理ポリシーを更新するので、携帯情報端末内のセキュリティ機能をリモートメンテナンスする

ことが可能である。

【0119】
【発明の効果】本発明によればフロントエンドOSの更新が必要であると判定された場合にバックエンドOSの制御下でフロントエンドOSの更新を行うので、情報処理装置のOSの更新を効率良く行うことが可能である。

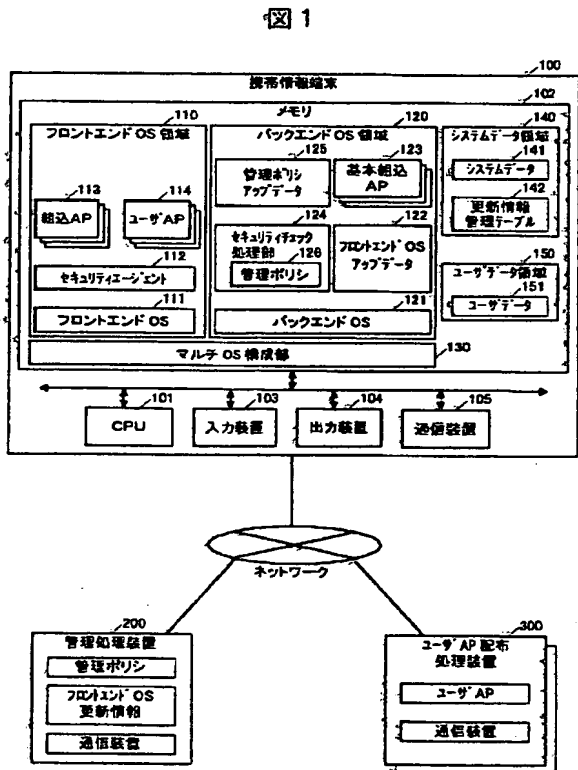
【図面の簡単な説明】

【図1】本実施形態の携帯情報端末マルチOSシステムの概略構成を示す図である。

【図2】本実施形態のフロントエンドOSアップデータ 122の処理手順を示すフローチャートである。

【図3】本実施形態の更新情報管理テーブル142の一例を示す図である。

【図1】



20

*【図4】本実施形態のセキュリティエージェント112の処理手順を示すフローチャートである。

【図5】本実施形態のセキュリティチェック処理部124の処理手順を示すフローチャートである。

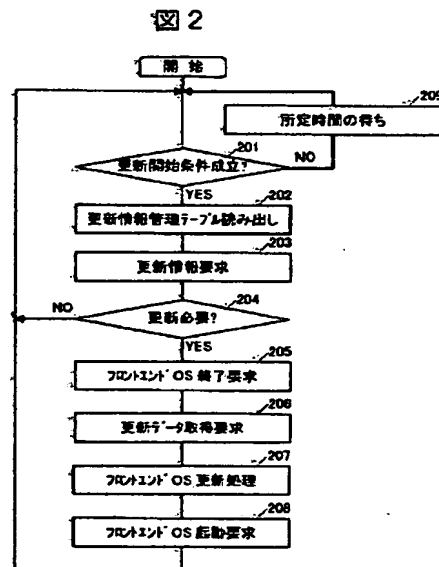
【図6】本実施形態の管理ポリシー126の一例を示す図である。

【図7】本実施形態の管理ポリシーアップデータ125の処理手順を示すフローチャートである。

【符号の説明】

100…携帯情報端末、200…管理処理装置、300…ユーザAP配布処理装置、101…CPU、102…メモリ、103…入力装置、104…出力装置、105…通信装置、110…フロントエンドOS領域、120…バックエンドOS領域、126…管理ポリシー、140…システムデータ領域、141…システムデータ、142…更新情報管理テーブル、150…ユーザデータ領域、151…ユーザデータ、111…フロントエンドOS、112…セキュリティエージェント、113…組込AP、114…ユーザAP、121…バックエンドOS、122…フロントエンドOSアップデータ、123…基本組込AP、124…セキュリティチェック処理部、125…管理ポリシーアップデータ、130…マルチOS構成部。

【図2】



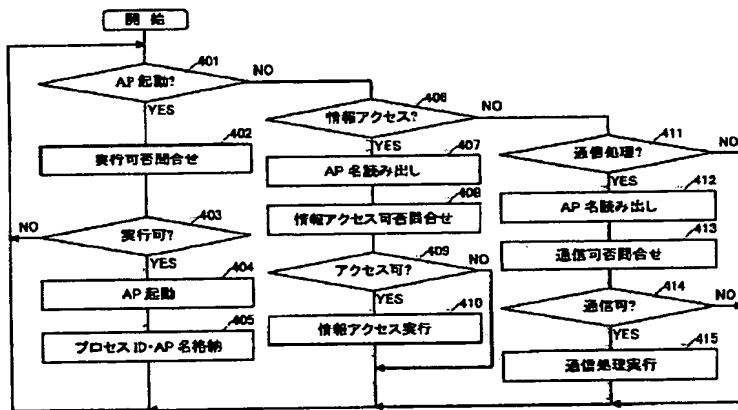
【図3】

図3

名称	バージョン	更新日付	格納形式	長さ	更新情報 取寄せ URL
フロント OS	3.02	2001.2.1	00000	1024	http://www.feos...
組込 AP 1	1.01	2001.7.1	00100	256	http://www.ap1...
組込 AP 2	2.31	2001.3.11	00200	512	http://www.ap2...
:	:	:	:	:	:

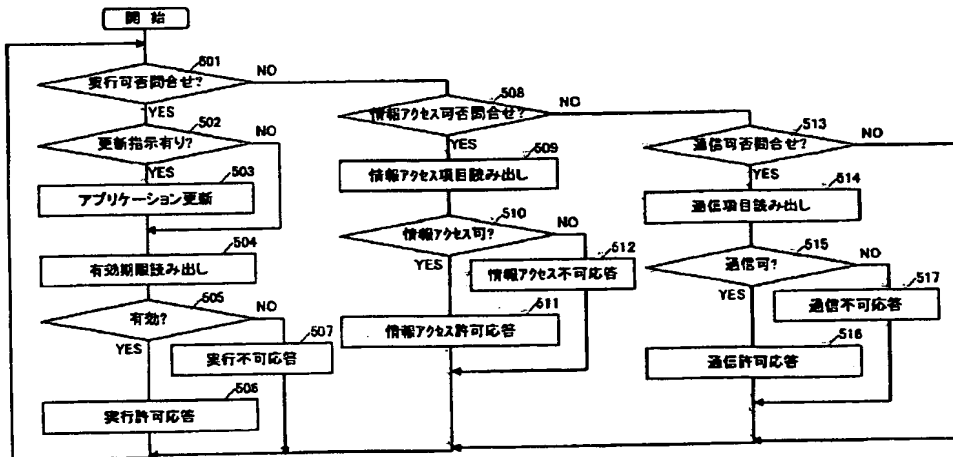
【図4】

図4



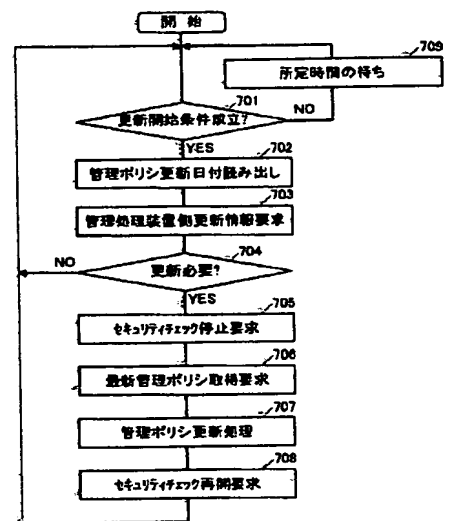
【図5】

図5



【図7】

図7



【図6】

図6

188

管理ポリシー 管理ポリシー取得先 http://www.policy 、更新日付 2001.10.1				
AP 名	更新指示	有効期限	情報カテゴリ	適否
AP1	無	2001.12.31	可	不可
AP2	有	2002.3.31	不可	可
：	：	：	：	：

フロントページの続き

(72)発明者 新井 利明
 神奈川県川崎市麻生区王禅寺1099番地 株
 式会社日立製作所システム開発研究所内

Fターム(参考) 5B076 AA02 AA13 EB02 FB00